

## UNITED STATES DISTRICT COURT

for the  
District of South Dakota

In the Matter of the Search of:

USA v. 22-40-05

Case No. 5:22-mj-51

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed (*identify the person or describe the property to be seized*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
 18 U.S.C. §§ 2251, 2252, 2252A

*Offense Description*  
 Distribution, Receipt, and Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.  
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.  
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

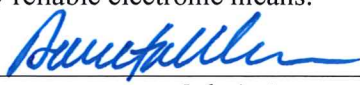
  
 Sarah B. Collins, AUSA

*Printed name and title*

Sworn to before me and: ☒ signed in my presence.

☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 3-23-22

  
*Judge's signature*

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate

*Printed name and title*

## UNITED STATES DISTRICT COURT

for the  
District of South Dakota

In the Matter of the Search of:

USA v. 22-40-05

)  
) Case No. 5:22-mj-51  
)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A as described in **ATTACHMENT A**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before April 6, 2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 3-23-22 2:15pmCity and state: Rapid City, SD

Judge's signature

Daneta Wollmann, U.S. Magistrate

Printed name and title

cc: AUSA Collins  
kle

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
WESTERN DIVISION

---

IN THE MATTER OF THE SEARCH OF: CASE NUMBER: 5:22-mj-51

USA vs. 22-40-05

**REDACTED**  
**AFFIDAVIT IN SUPPORT OF**  
**SEARCH WARRANT**  
**APPLICATION**

---

State of South Dakota    )  
  ) ss  
County of Pennington    )

I, Brian Freeouf, Special Agent with the South D and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

1. I began my law enforcement career with the Pennington County Sheriff's Office in July of 2005. I spent approximately 3 years on patrol in the contract community of Wall, SD. I was then assigned to the patrol division in Rapid City in 2008. I was promoted to the rank of Senior Deputy, in July of 2010. I also spent time as a School Liaison Officer and Criminal Investigations Division as a Property Crimes Investigator. Even though I was assigned as a Property Crimes investigator I also investigated other crimes but not limited to homicides, rapes, assaults, and coroner duties. My other assignments within the Sheriff's Office include Deputy Coroner, Field Training Deputy, and Defensive Tactics Training Administrator. Since November of 2014 I have been assigned to the ICAC Task Force (Internet Crimes against Children). The investigations worked by this unit include child pornography, solicitation of minors, sexual

exploitation of minors, disseminating harmful materials to minors, and human trafficking. Since January of 2020 I have been hired by the South Dakota Division of Criminal Investigations as a special agent. I am still assigned to the ICAC Task Force and continue investigations as listed above.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statutes 18 U.S.C. § 2251, 2252 and 2252A, involving violations of law involving child pornography. During my law enforcement-career I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, including by computer or utilizing the internet.

4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training



and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. The undersigned respectfully requests that a search warrant be issued to permit a search of one Dell D075 desktop computer, serial number VNWFA00, with a 500 GB Seagate hard drive, serial number Z6EA1DK9 and one Hewlett Compaq 6530b laptop computer, serial number CNU008357Q with a Hitachi HDD, 160 GB hard drive, serial number 100210PB5B01QCF6YJKG (hereinafter also referred to as SUBJECT DEVICES) and further, to access and search the contents of said electronic device without seeking an additional or separate warrant. Both SUBJECT DEVICES were previously seized and searched by law enforcement and have remained in secure custody since that time.

6. The warrant is sought in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, which criminalize the production, distribution, receipt and possession of child pornography.

DEFINITIONS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services

allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. *Computer*: The term “computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware*: The term “computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections),



as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices*: The term “computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. *Computer-Related Documentation*: The term “computer-related documentation” means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software*: The term “computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service* (“ESP”): as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

m. *File Transfer Protocol* (“FTP”): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet*: The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection*: The term “Internet connection” means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor*: The term “minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service* (“RCS”): as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service* (“SMS”): as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium*: The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions*: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. *Wireless Network*: The term “wireless network” means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

#### PROBABLE CAUSE

8. On Saturday, June 08, 2019, I was conducting an online investigation on the BitTorrent network for offenders sharing child pornography.

An investigation was initiated for a device at IP address 209.159.236.231, because it was associated with a torrent with the infohash: 7519c5b8d7d6a41dfed353b7e42687b4e1ecbbfb. This torrent file contained 81 files, at least one of which was suspected child pornography. IP address 209.159.236.231 belonged to Michael Wilkes during all relevant times.

9. Using a computer running investigative BitTorrent software, my computer made a direct connection to a device utilizing Wilkes' IP address. The device was using BitTorrent client software -UT355W- µTorrent 3.5.5.

10. On Saturday, June 08, 2019, between 9:01 p.m. and 10:32 p.m., I successfully downloaded 27 files made available by a device utilizing Wilkes' IP address. That device was the sole candidate for each download, meaning that each file was downloaded directly from Wilkes' IP address.

11. On Sunday, June 09, 2019, I was again conducting an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device using the same IP address 209.159.236.231, because it was associated with a torrent with the infohash: 989939150d4e563560fc93667029d764e9eea064. This torrent file contained 176 files, at least one of which was suspected child pornography.

12. Using a computer running investigative BitTorrent software, my computer made a direct connection to a device using Wilkes' IP address. That device was using BitTorrent client software -UT355W- µTorrent 3.5.5.

13. On Sunday, June 09, 2019, between 4:34 p.m. and 5:30 p.m., I successfully downloaded 1 file that the device utilizing Wilkes' IP address was

transporting. That device was the sole candidate for the download, meaning the file was downloaded directly from Wilkes' IP Address.

14. On both days partial downloads were also completed from files contained within the above listed Torrents. It should be noted that I considered many of the videos to be age difficult, meaning it was possible they were child pornography, but the people depicted could also be over 18 years old. Those downloads are further described as follows:

**File:** 2019-06-08\_21-01-19\_1\Download\Stickam Captures - 2010-01\datimeis1202-2.avi **Category:** Child Pornography

**Video Length:** 02:24

**Description:** This video shows what appears to be a 10-14-year-old girl. Throughout the video she is sitting in front of a web camera. There is a closeup video of her bare vagina. She touches her vagina and inserts a glue stick into her vagina throughout the video. The girl also exposes her bare breasts and nipples during the video.

**File:** 2019-06-09\_16-34-26\_2\Download\STICKAM\babygrly\baby\_gurly04.wmv

**Category:** Child Pornography

**Video Length:** 00:14.36

**Comments:** This video shows three girls approximately 12-15-year-old girls. One of the girls is completely naked and stands in front of what appears to be a webcam. The girl's bare vagina, breasts, and nipples are exposed in this video.

**File:** 2019-06-09\_16-34-26\_2\Download\STICKAM\babygrly\baby\_gurly03.wmv

**Category:** Child Pornography

**Video Length:** 00:15.15

**Comments:** This video appears to be of the same girls as listed in the last video. All appear to be 12-15 years old. Throughout the video two of the girls show their bare breasts and nipples. One of the girls stands completely naked in front of the camera except she is covering her vagina with a stuffed penguin. That girl eventually removes the penguin exposing her bare vagina. One of the girls also sucks on a cylindrical shaped object making it look like she is performing oral sex on a male's erect penis.

15. During my investigation, I was able to find the above IP address 209.159.236.231 was provided by Vast Broadband. I submitted a subpoena to



Vast Broadband for any subscriber or user information associated with that IP address. Vast responded with the following information:

Michael Wilkes

[REDACTED]

Summerset, SD 57718-0000

478-954-7490

[bowtiemnmt@aol.com](mailto:bowtiemnmt@aol.com)

16. Once I was aware of this information, I recalled a prior investigation in which I engaged in 2017, case number 17-104305. At that time, I made a download from a user with the same user subscriber information was given to me through vast broadband associated with the 2019 downloads described above. The following are the details from that case:

17. On Saturday, July 29, 2017, I was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device at IP address 67.158.10.113, Wilkes' IP address, because it was associated with a torrent with the info hash: 4744fa4b8fc41d672d52ec313edda713c5fab178. The torrent file contained one suspected image of child pornography.

18. Using a computer running investigative BitTorrent software, my computer made a direct connection to a device utilizing Wilkes' IP address. The device was using BitTorrent client software -UT3500- µTorrent 3.5.

19. On Saturday, July 29, 2017, between 7:25 p.m. and 7:36 p.m., I successfully downloaded one file made available by a device utilizing Wilkes' IP address. That device was the sole candidate for the download, meaning the file was downloaded directly from Wilkes' IP address.

20. I also downloaded files from this IP address on 6/17/17, 7/09/17, 07/30/17, and 08/03/17. The files contained age difficult images and videos as well as images and videos of child pornography. Some of the videos and images meet the South Dakota definition of child pornography but not the federal definition. The following is a sample of some of the child pornography downloaded:

**File:** 2017-07-29\Download\(\Pthc) 13Yo Boy And 13Yo Lolita Girl Having Sex.mpg

**Category:** Child Pornography

**Video Length:** 00:13.17

**Comments:** The video starts with a boy and a girl kissing on a bed. Based on the title of the video and the way the two appear, I would estimate both were around 13 years old. The girl is wearing a bra and small shorts and the boy is wearing underwear. At 3 minutes the girl has the boy's bare penis in her mouth and is licking it. At 9min 30sec, the boy is vaginally penetrating the girl with his erect penis while she is on her back. At this point and time both boy and girl are completely naked. At 11min the boy is still vaginally penetrating the girl with his erect penis. At 13min the boy pulls his erect penis out of the girl's vagina and ejaculates on her stomach. This video is in violation of SDCL: 22-24A-3 Possessing, Manufacturing, or Distributing child pornography.

**File:** 2017-06-17\Download\webcam\_loli\_13\_video\Acegirl.webm\_thumbs.jpg

**Category:** Child Pornography

**Video Length:** Image

**Comments:** This is a collage of images of a girl approximately 10 to 13 years old. The images in the collage show her exposing her bare breasts and nipples, her bare vagina, and her masturbating.

**File:** 2017-07-09\Download\pedo-stars Dee\_and\_Desi\(\Pthc) Dee & Desi (Fv2007) - 13Yo Girls And Boys.avi.jpg

**Category:** Child Pornography

**Video Length:** Image

**Comments:** This is a collage of images which appear to have 10 to 15-year-old boys and girls in the images. The boys and girls are naked in the images. Some of the images has a girl either stroking the boy's erect penis or performing fellatio on the boy. Bare penis, vagina, and breasts are visible throughout the images.

**File:** 128-0 G:\2017-07-30\Download\STICKAM SuperPack (71 Videos)\bri\_bear.avi

**Category:** Child Pornography

**Video Length:** 00:09.32

**Comments:** This video was of an approximately a 12 to 16-year-old girl. Throughout the video she shows her bare vagina, breasts, and nipples. At one point the girl lays on a bed and inserts the handle of a hairbrush into her vagina. This happens multiple times throughout the video.

**File:** 2017-08-03\Download\ (Pthc) Boy Sister Incest Brazil\ (Pthc) Boy Sister Incest Brazil.mpg

**Category:** Child Pornography

**Video Length:** 00:07.53

**Comments:** This video was of a girl and boy both approximately 12 to 15-years-old. The video starts with the girl naked exposing her bare breasts, nipples, and vagina. The boy and the girl are then naked together on a bed while the girl preforms fellatio on the boy. The boy then inserts his penis into the girl's vagina. The boy eventually pulls his erect penis out of the girl and ejaculates on her stomach.

21. Due to case load and other commitments, I was unable to immediately investigate the 2017 downloads. On July 12, 2018, Michael agreed to meet with Detective Elliott Harding and me at Dunn Brothers coffee in Rapid City. We introduced ourselves to Michael and we told him how we were employed. Michael confirmed he lived in his house for the past three years. He only lives with his disabled wife. People do come to visit but not during the duration of the online activity I was investigating. Michael confirmed he had his internet through Vast/Knology and that the router was passcode protected.

22. Michael advised he has looked at pornography but was unsure if he had ever seen child pornography. Michael was unable to give me a definition of child pornography. I explained it to him, but he still claimed that he was unsure if he had ever seen child pornography. I told Michael that because the downloads came from his house, and it was only his wife and him who lived there, we believed he was the one downloading the child pornography. Michael denied this

multiple times. I asked Michael if we could examine his devices with his permission to help clear his name. Michael said he would have to think about that. Michael eventually said he wanted legal counsel from a lawyer. At that point the interview ended, and we left from the coffee shop.

23. On August 28, 2019, the Honorable Judge Gordon Swanson granted a search warrant for the residence at [REDACTED], Summerset, SD 57718. On August 29, 2019, the Honorable Judge Robert Gusinsky granted a search warrant for Michael Wilkes, his work address of [REDACTED], Rapid City, SD. 57702, and his vehicle.

24. On August 29, 2019, both search warrants were executed. We executed the house warrant first and we seized multiple devices. While at the house, I briefly spoke with Michael's wife. She indicated he told her about the last time we spoke with him about child pornography. She also told other Agents that Michael's computers were downstairs. She said she had not been downstairs in a long time because she cannot walk up and down stairs very well. Michael's wife indicated she did not want to talk to us any further about the issue.

25. Once we were done executing the search warrant at the house, then DCI SSA Brent Gromer, RCPD ICAC Detective Elliott Harding, and I went to Wilkes' work and met with him in his office at about 9:15 a.m. Gromer, Harding and I were shown to Wilkes' office and spoke with him. I asked Wilkes if remembered Detective Harding and I and he indicated he did. I told him there was another issue at his house and we had search warrant for his house. I gave

Wilkes a copy of the warrant and allowed him to review it. He asked what the investigation was regarding. I told him there were more child pornography downloads from the bit-torrent network associated with his IP address. I reminded him it was the same conduct we spoke with him about previously. I read Wilkes his Miranda Warning and asked if he wanted to talk about the incident, to which he said "no" but thereafter asked if I could give him some more information.

26. I told Wilkes that in June 2019 someone utilized his IP address to download child pornography. I asked him if anyone was staying with them at their house. Michael looked at his calendar and indicated that no one stayed at his house. I told Michael we had already executed a search warrant at his residence and took all of his devices. I then advised him the second search warrant we had was for his cell phone and any personal devices he had with him or in his car. He gave us his cell phone and advised his passcode was his date of birth. I told Michael we found a program on one of his computers which was consistent with the program used to download child pornography. I told him he did not have to answer my question, but did he have an explanation for it. He just said, "it may very well be". I asked if his internet was passcode protected and he indicated it was. He also said if anyone came over to his house, they could use the internet. I asked again if anyone was at his house in June. He did not indicate anyone was at his house in June. I asked Michael if he wanted to tell us about speaking to his wife after the last time we had spoken. Michael said he told her he did not download any child pornography. We all went to the

parking lot and Detective Harding and I searched Michael's car and we found nothing of evidentiary value.

27. All items seized from his house and work were taken back to the ICAC lab for examination. ICAC Forensic Examiner Hollie Strand conducted exams on multiple items, locating numerous images of child pornography on two devices – Item 1 (Toshiba Satellite Laptop) and Item 7 (Hewlett Packard Compaq Laptop). She examined the SUBJECT DEVICES and originally determined there was nothing of evidentiary value contained therein. While preparing for trial, Strand recognized that Wilkes was using certain devices to conduct his regular business and others to access and/or collect child pornography. It appears the SUBJECT DEVICES were his clean devices. They are of evidentiary value because using multiple devices for different purposes, legitimate vs. illegal, at the same time indicates knowledge regarding his criminal activity.

28. Strand saved her original extractions of the SUBJECT DEVICES on an external hard drive, which later corrupted rendering the content inaccessible. Thus, she will need to reimage those devices and seeks this warrant to do so.

BACKGROUND ON CHILD PORNOGRAPHY,  
COMPUTERS, THE INTERNET, AND EMAIL

29. I have training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other.



Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer

protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Based upon my training and experience, as well as information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and

storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during a search of physical premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

**Your affiant wishes to draw the Court’s attention to the following facts regarding inferences from the above-mentioned facts that are based upon my knowledge, training and experience:**

31. I am aware that often times, even persons who know they are under investigation for internet crimes, will not discontinue their criminal conduct. Sometimes this is because they believe they will outsmart the investigators through their computer knowledge, or because they are addicted to their criminal conduct, or if they believe they have gotten away with their prior internet crimes due to the passage of time since the inception of the investigation.

32. Through my training and experience, I am aware people involved in the online exploitation of children, especially those who are computer-savvy, may use cloud services and may have multiple devices which access the cloud storage device. This may be accomplished utilizing a cell phone, tablet, computer, or other device which has access to the internet.

33. I know that individuals who are involved in the online exploitation of children will often store evidence of their exploitation on their computer system. I also know that when an individual utilizes multiple storage systems, there is often evidence of child exploitation stored in multiple locations.

34. I know that electronic and/or written communication may exist on the computer system, demonstrating the access to an app or website used for the exploitation of minors. I know that exchanging images during chats, such as photos of the offender sent to the minor or vice versa, frequently causes the displayed images to be saved to the hard drive of the computer or in the "images" or "photos" file on a smart phone or tablet. The device may store the images even if the user believes them to be deleted.

35. I know that people involved in the online exploitation of children typically associate online with other people with similar deviant sexual interests in children. Accordingly, remnants of communications between the offender and other offenders are commonly found on the user's device(s).

36. I know that people who use personal computers in their homes tend to retain their personal files and data for extended periods of time; months or even years. Due to a personal computer's unique ability to store large amounts



of data for extended periods of time without consuming much additional physical space, people tend to retain this data. Affiant knows this to be true regardless of whether or not a person has traded-in or "upgraded" to a new personal computer. Personal computer users routinely transfer most of their data onto their new computers when making an upgrade. This data transfer is often done by saving files from the old computer to media sources (CD's or floppy disks, etc.) and then saving them to the new hard drive. Any evidence of online exploitation of minors is as likely as other data to be transferred to a person's new, replacement, or upgraded computer system.

37. I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools.

38. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may

access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

39. Based on my training and experience, I know that data can be received by use of a home computer and transferred to other electronic devices, such as a cell phone. I also know that data or images can be received by use of a cell phone and transferred to a home computer.

40. Based on my training and experience, as well as my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

41. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable

evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A  
SEXUAL INTEREST IN CHILDREN AND/OR WHO PRODUCE,  
RECEIVE AND/OR POSSESS CHILD PORNOGRAPHY

42. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines,

correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are highly valued.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.




LIMIT ON SCOPE OF SEARCH


43. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION


44. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, are located on the SUBJECT DEVICES, described further in Attachment A.

45. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

  
Special Agent Brian Freeouf  
Internet Crimes Against Children  
Taskforce

SUBSCRIBED and SWORN to  
 in my presence  
\_\_\_\_\_ by reliable electronic means

this 23rd day of March, 2022.

  
DANETA WOLLMANN  
U.S. MAGISTRATE JUDGE

**ATTACHMENT A**  
**Property to Be Seized and Searched**

1. One Dell D075 desktop computer, serial number VNWFA00, with a 500 GB Seagate hard drive, serial number Z6EA1DK9; and
2. One Hewlett Compaq 6530b laptop computer, serial number CNU008357Q with a Hitachi HDD, 160 GB hard drive, serial number 100210PB5B01QCF6YJKG.